

NetDiligence®

RANSOMWARE

2021 SPOTLIGHT REPORT



OUR SPONSORS



RSM



Table of Contents

Introduction.....	1
Key Findings for 5-Year Period 2015–2019.....	2
SMEs – Costs for All Ransomware Claims.....	2
SMEs – Costs for Claims Where Ransom Demand is Known.....	3
Large Companies – Costs for All Ransomware Claims	4
Looking at the Numbers	5
Ransomware Year by Year	5
The Growing Cost of Ransomware.....	5
Yearly Average and Median Costs	5
Business Interruption	6
To Pay or Not to Pay	6
Organization Size.....	6
Ransom Paid vs Not Paid.....	6
Average Costs by Organization Size	6
Business Sector	7
Average Costs by Sector.....	7
Encryption vs Extortion and Leak Sites.....	8
The Law Enforcement Perspective.....	8
Ransomware in 2020.....	8
OFAC Advisory on Ransomware	9
What Can You Do?.....	9
Conclusion.....	9
Graphical Views of the Data.....	10
Histograms.....	10
Ransom Amounts (Log ₁₀)	10
Crisis Services Costs (Log ₁₀).....	11
Total Incident Cost (Log ₁₀).....	12
Correlations	13
Does the ransom demand correlate with annual revenue?.....	13
Does the incident cost correlate with annual revenue?.....	14
Does the business interruption cost correlate with ransom demand?.....	15

Introduction

NetDiligence® is pleased to present this updated spotlight report on a most timely topic – ransomware. This analysis is based on more than 900 cyber insurance claims for ransomware incidents.

Since the publication of our initial *Ransomware Spotlight Report* in January 2020, the losses caused by ransomware incidents have impacted every sector of every economy. Healthcare, Professional Services, Manufacturing, and Retail are the sectors at the apex of financial impact. Cyber insurers have seen their loss ratios increase dramatically, and, as a result, are actively working with their cybersecurity technical partners and reinsurers on more stringent loss control requirements and underwriting procedures to better control this growing threat.

The term “ransomware” came into the cyber lexicon approximately a decade ago. While there is no universally accepted definition of the term, it is useful to think of it as a network intrusion that often begins with a phishing attack that dupes an employee into unintentionally installing malware that encrypts systems throughout the enterprise. Modern variants also exfiltrate sensitive data to increase pressure on the victimized organization. An extortion demand is then made.

Since 2017, the average ransom demand has increased from \$15K to \$175K – an almost twelve-fold increase. Ransom demands crossed the \$1M threshold in 2018 and the \$3M threshold in 2019. Publicly available information indicates that ransom demands crossed the \$30M threshold in late 2020 (although in reality these demands are often negotiated downwards, sometimes quite significantly). Ransom demands have increased to the point that there is sometimes insufficient capacity in on-demand Bitcoin and other cryptocurrency exchanges to meet ransom demands in a timely manner.

The analysis in this spotlight report is based on data for over 900 ransomware incidents in the NetDiligence claims database. These incidents, all provided by NetDiligence’s insurance partners, date from 2015-2019.

Incidents at small to medium enterprises (SMEs) account for almost all the ransomware claims (N=915). Because the dataset does not yet contain incidents that occurred in 2020 (due to our claims data collection schedule), we have supplemented the data analysis using anecdotal evidence from private and public sources.



Key Findings for 5-Year Period 2015–2019

SMEs – Costs for All Ransomware Claims

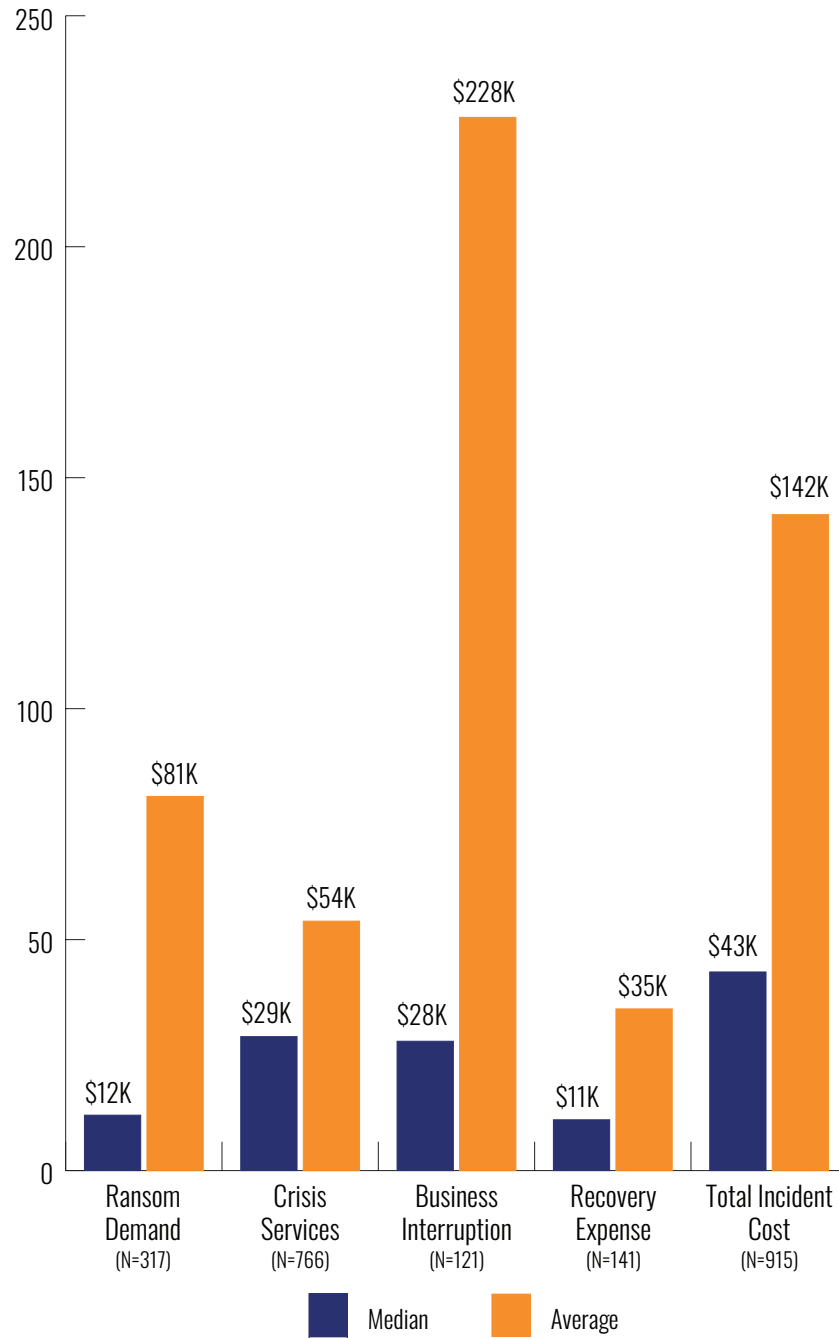


Figure 1

SMEs – Costs for Claims Where Ransom Demand is Known

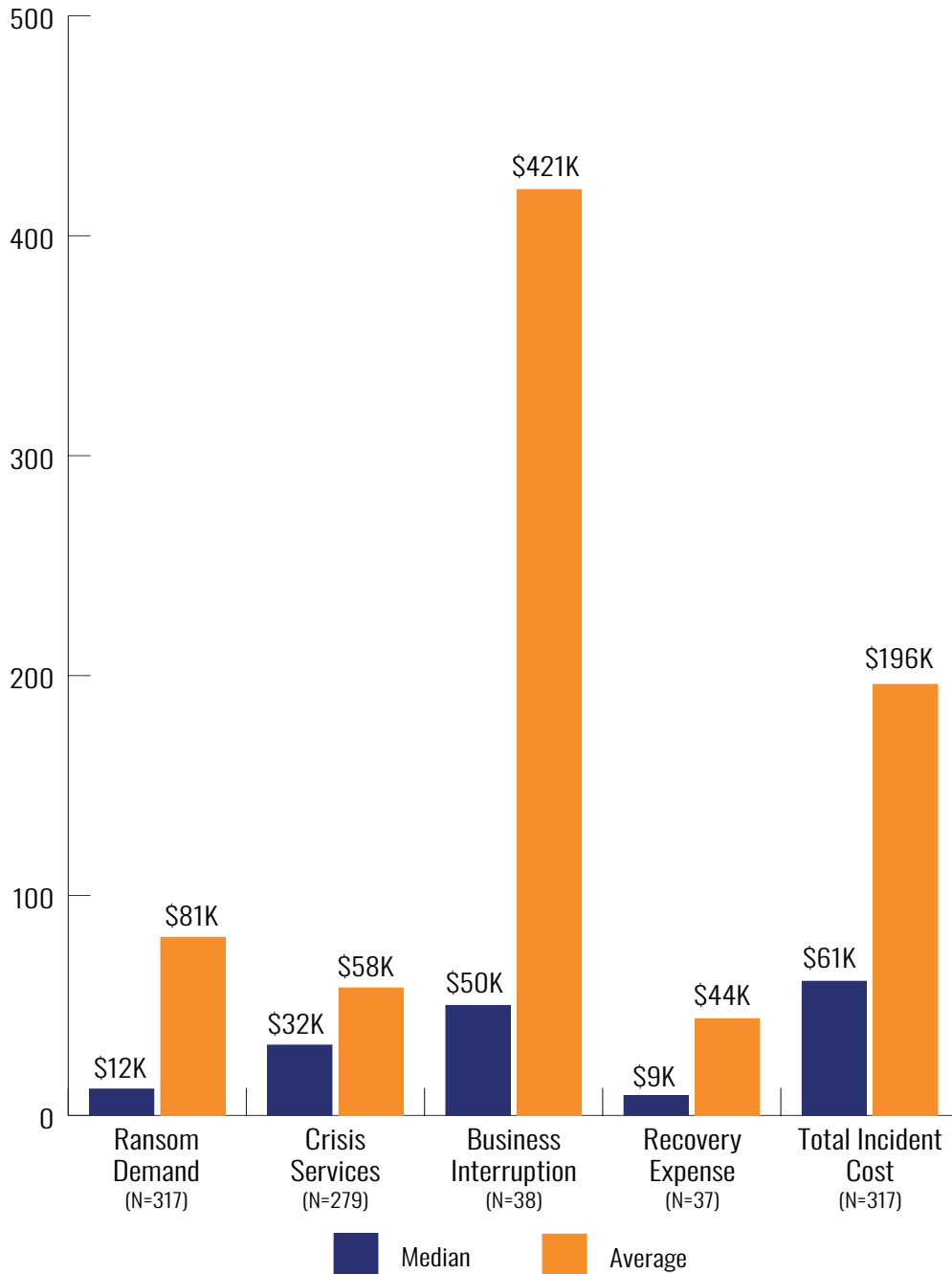


Figure 2

Note: Ransom amounts were provided for about one third of incidents. The costs of incidents where the ransom was provided are higher than the overall costs. There was no data for Large Companies.

Large Companies – Costs for All Ransomware Claims

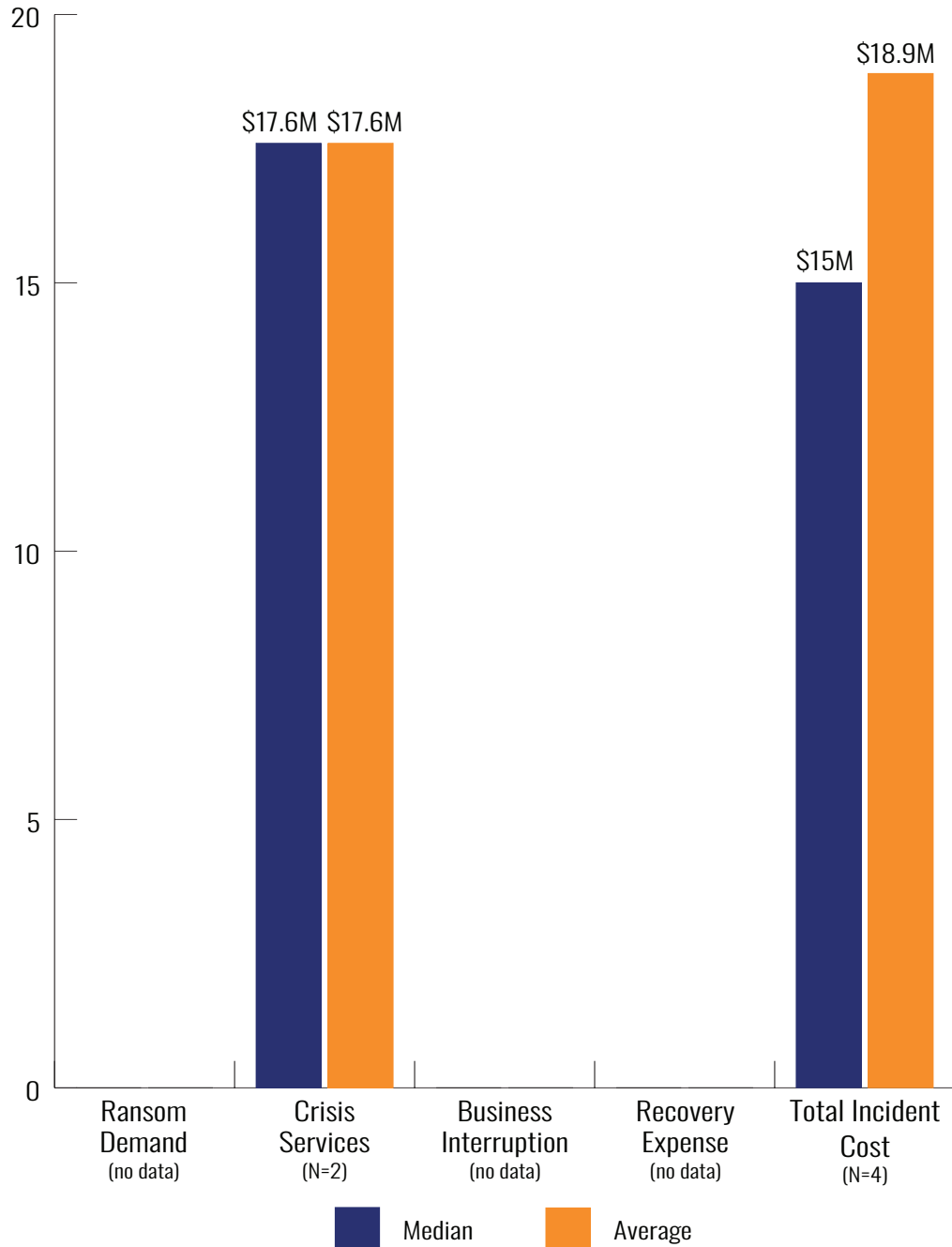


Figure 3

Looking at the Numbers

Ransomware Year by Year

It is no secret that ransomware incidents have increased dramatically in both frequency and magnitude since 2015. For 2020, while we have not yet collected and analyzed the data, we know from

insurers and incident responders that the numbers have gone off the charts. One incident responder reported dealing with almost 100 ransomware incidents in October alone, with several ransom demands in the millions and even tens of millions of dollars.

The Growing Cost of Ransomware

Based on 317 Claims Where Both Ransom Demand and Total Incident Cost are Known

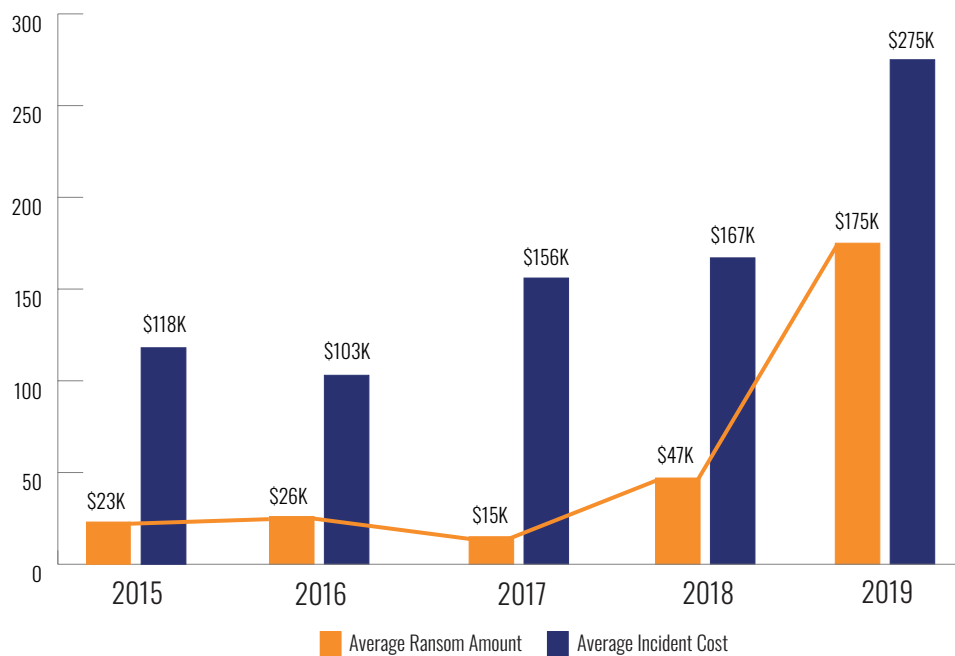


Figure 4

Yearly Average and Median Costs

Year	Claims	Ransom Demand		Incident Cost	
		Average	Median	Average	Median
2015	8	23K	3K	118K	40K
2016	19	26K	12K	103K	90K
2017	79	15K	7K	156K	46K
2018	103	47K	7K	167K	41K
2019	108	175K	26K	275K	100K
2015-2019	317	81K	12K	275K	61K

Table 1

Business Interruption

Ransomware incidents often cause significant loss due to business interruption (BI). The dataset contains 121 SME claims (2015-2019) that provided numbers for BI. The average BI amount was \$228K (median=\$28K; max=\$5.1M). The average incident cost for these claims was substantially higher than the overall average incident cost: \$342K vs \$142K (median=\$85K; max=\$6.6M).

As can be seen in the linear regression graph at the end of this report, there is no apparent correlation between ransom demand and business interruption cost. In one claim, a negligible ransom demand (300 dollars) caused a \$5M business interruption loss and a \$6.6M total incident cost.

To Pay or Not to Pay

Some organizations can recover from a ransomware incident without paying the ransom. They do this by utilizing uncorrupted backups, reverse-engineering decryption keys, acquiring the decryption key from another source such as the FBI, re-creating lost data, and/or replacing compromised systems with new ones.

The NetDiligence data shows that costs to organizations that do not pay a ransom demand are higher—sometimes significantly—than costs to organizations that do pay the demand.

Ransom Paid vs Not Paid

	Ransom Paid		Ransom NOT Paid		Variance
	Claims	Average	Claims	Average	
Crisis Services	709	53.5K	57	54.2K	1%
Business Interruption	113	192K	8	730K	280%
Recovery Expense	134	28K	7	94K	231%
Total Incident	852	140K	64	183K	31%

Table 2

Organization Size

The average estimated revenue (organization size) for ransomware victims was \$70M (N=356; median=\$20M, max=\$1.6B).

When segmented by revenue size, the averages are as follows:

Average Costs by Organization Size

	Claims	Ransom Amount	Crisis Services	Total Incident Cost
Nano-Rev (<\$50M)	409	56K	55K	95K
Micro-Rev (\$50M-\$300M)	122	148K	106K	303K
Small-Rev (\$300M-\$2B)	27	499K	125K	733K

Table 3

As can be seen in the linear regression graphs at the end of this report, there is no apparent correlation between ransom demand and company size or ransom demand and total incident cost.

Business Sector

Organizations in every sector of the economy have been victimized by ransomware attacks. The table below, based upon data from 2015-2019, tells the story. The greatest number of claims occurred in

Healthcare, followed by Professional Services. Highest average costs occurred in Manufacturing, followed by Entertainment.

Average Costs by Sector

	Claims	Ransom Amount	Crisis Services	Total Incident Cost
Healthcare	312	26K	35K	107K
Professional Services	200	43K	50K	88K
Manufacturing	65	305K	47K	490K
Retail	50	82K	48K	130K
Nonprofit	42	82K	105K	105K
Technology	31	142K	94K	221K
Financial Services	31	27K	48K	62K
Education	29	219K	83K	202K
Public Entity	28	153K	114K	140K
Transportation	21	62K	67K	138K
Energy	6	33K	70K	57K
Hospitality	5	23K	41K	52K
Telecommunications	5	7K	86K	96K
Restaurant	3	n/a	45K	143K
Entertainment	2	152K	84K	480K
Media	2	1K	39K	40K
Other	83	98K	74K	156K

*sorted by the number of claims

Table 4

Ransomware in 2020

There have been too many notable ransomware incidents in 2020 to list all of them, but examples* of some that were publicly reported are:

- Cognizant, April, 2020 – estimated impact on Q2 margins: \$50M-70M
- Magellan Health, April, 2020 – ransom demand and data exfiltration affecting as many as 1.7M people
- Carnival Corporation, August, 2020 - ransom demand and data exfiltration
- Canon Corporation, August, 2020 – ransom demand and data exfiltration
- Foxconn, November, 2020 – \$34M ransom demand, data encrypted, backups deleted
- Habana Labs, December, 2020 – ransom demand, data exfiltration, data leaked online
- Randstad, December, 2020 – data exfiltration, data leaked online

The frequency of attacks and the size of the ransom demands have grown dramatically in 2020, and it appears that the situation is only going to get worse in 2021.

** It should be noted that none of these examples were represented in our dataset.*

Encryption vs Extortion and Leak Sites

Ransomware incidents are no longer just about encrypting files and responding to a demand for payment. In mid-2019, security experts, incident responders, and breach response lawyers began talking about ransom demands being the last step in a lengthy exploit: bad actors infiltrated systems, moved laterally through a network for months, exfiltrated data at leisure, and at the very end, encrypted the enterprise network/data. They then made a ransom demand for a decryption key, or for a promise not to publish stolen data, or both. Expert consensus suggests that attackers may persist in a network for as long as eight months before making their presence known to the victim.

An even newer emerging trend involves the exfiltration of data and extortion. Attackers sometimes do not even take the trouble to encrypt the data. After exfiltration, they issue an extortion demand – pay up or your data will be exposed. Sometimes, to prove that they have the data they are talking about, they will send the victim a subset of data or even publish some of it online. If the extortion demand is not met, additional confidential data may be exposed or auctioned off to the highest bidder.

Leak sites are sites operated by malicious actors where stolen data is exposed and auctioned off. A few of these sites are:

- Data Leak Blog
- CLOP^–LEAKS
- Dopple Leaks
- Corporate Leaks

For more information about how stolen data is marketed by criminal groups, see this blog published by Cyware: [Data Dumping by Ransomware Operators: Where and How do They Leak?](#)"

The Law Enforcement Perspective

The FBI and other law enforcement entities have an important role to play in ransomware incidents, and under most circumstances should be notified immediately.

Law enforcement considers its mission to be the apprehension and punishment of criminals and not the punishment of victims. Except when required in court proceedings, they strive to maintain strict confidentiality when investigating and prosecuting a ransomware incident.

The position of the FBI is that victims should not pay ransoms. However, the FBI understands that, as a practical matter, victims may not have an alternative. They are often a great resource for victimized organizations, working with Breach Coach® counsel to provide guidance as needed.

OFAC Advisory on Ransomware

On October 1, 2020 the Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Ransomware Advisory | U.S. Department of the Treasury).

In brief, the Advisory states that entities that make payments to sanctioned persons or entities may be subject to civil enforcement actions, whether such payments were made knowingly or unknowingly.

The following excerpt from the Advisory highlights mitigating actions that victim entities might take:

"As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome."

It is still early to know how OFAC will proceed in these matters. As always, the best course of action is to

seek the advice of experienced incident response (IR) experts, cryptocurrency vendors, and Breach Coach® legal counsel. Many cyber insurers list the IR and legal experts they rely upon to help policyholders with ransomware inside their eRiskHub® portals.

What Can You Do?

There are actions that organizations can take to mitigate the impact of ransomware incidents, and even prevent them. Rather than present a long list, we will just mention a few. All of the items listed here should be components of a sound information security program (but not necessarily the entirety of such a program).

- Protect credentials, especially IT administrative ones. Consider implementing multi-factor authentication (MFA). By compromising credentials, malicious actors often gain root access to your infrastructure.
- Implement next-generation endpoint protection that combines AI-based prevention technologies with full attack visibility so you can stop ransomware attacks before they disrupt your business
- Implement proper network segmentation. Isolate administrative functions from operational functions.
- Do backups correctly and rigorously; have at least two sets of backups that cannot be reached via the network. Consider cloud-based backup and traditional "air gap" off-premise physical storage solutions. Also consider multi-versioning (i.e., keeping multiple-dated backup images), as well as Write-Once, Read-Many (WORM) solutions. Conduct regular integrity and recovery testing of backups. In the end, your backups will not save you if they are compromised..
- Be serious about security awareness training. Repeat the training on a regular basis and test users.
- Implement and test, regularly, an incident response plan.
- Isolate a hot or cold backup site as much as possible and test regularly.

Conclusion

We hope you have found this *Ransomware Spotlight Report* informative and enjoyable to read. Please visit our website (<https://netdiligence.com>) for other Spotlight reports as well as our annual Cyber Claims Studies.

Graphical Views of the Data

Histograms

Ransom Amounts (Log₁₀)

5-Years: 2015–2019
(N=317)

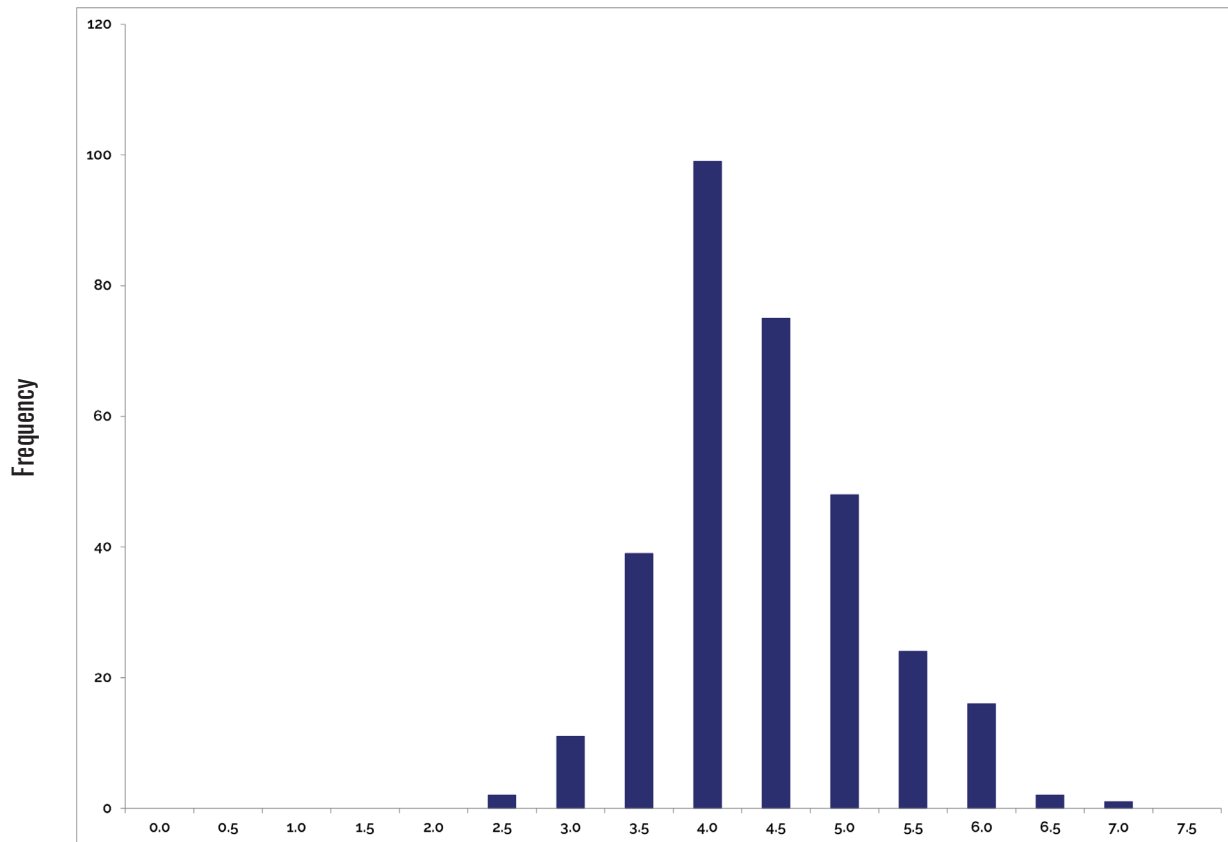


Figure 5

Crisis Services Costs (Log₁₀)

5-Years: 2015–2019
(N=766)

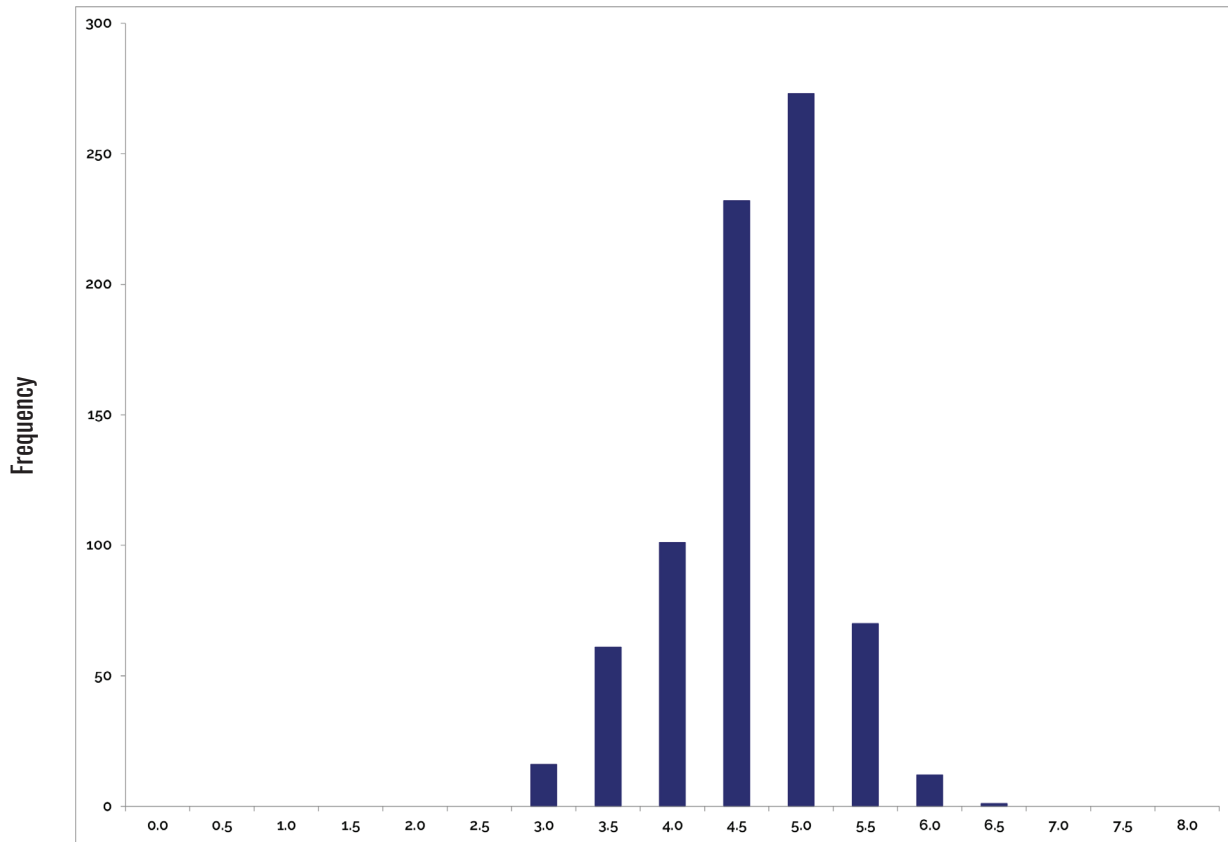


Figure 6

Total Incident Cost (Log₁₀)

5-Years: 2015–2019
(N=916)

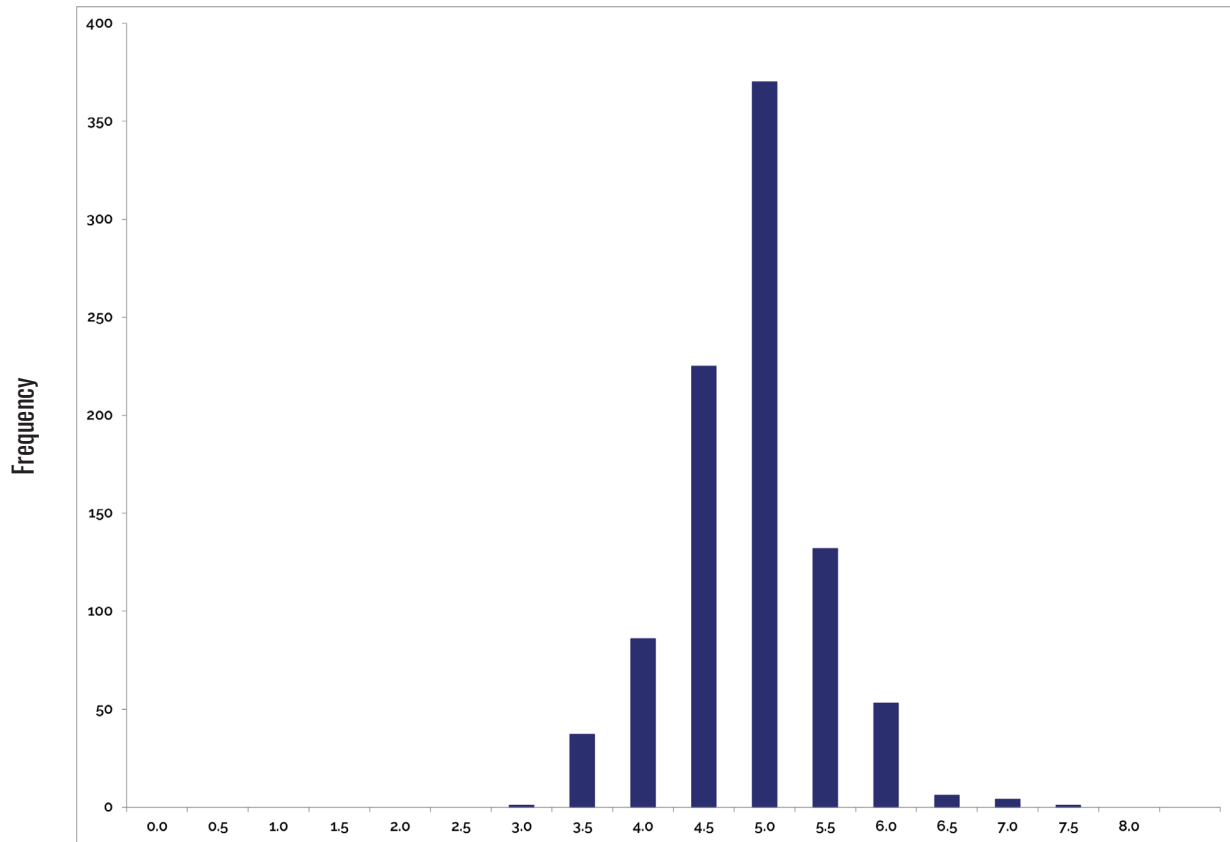
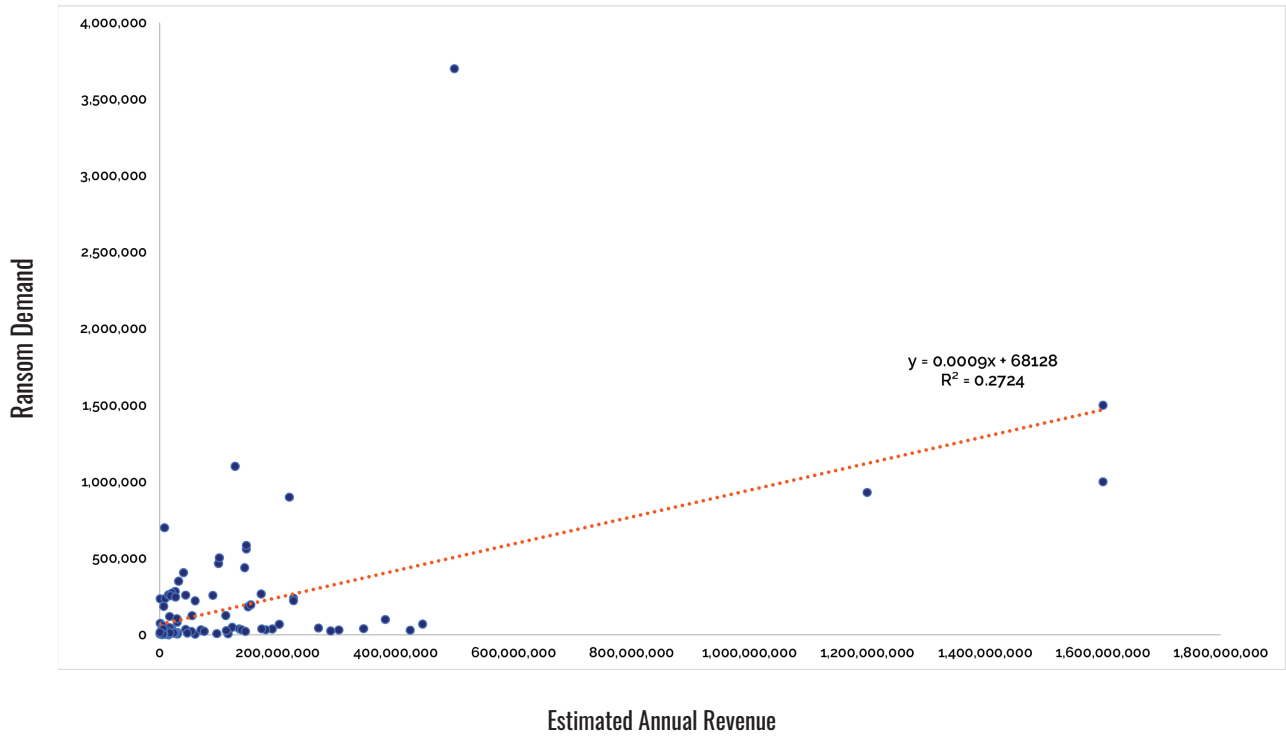


Figure 7

Correlations

Does the ransom demand correlate with annual revenue?

5-Years: 2015–2019
(N=126)

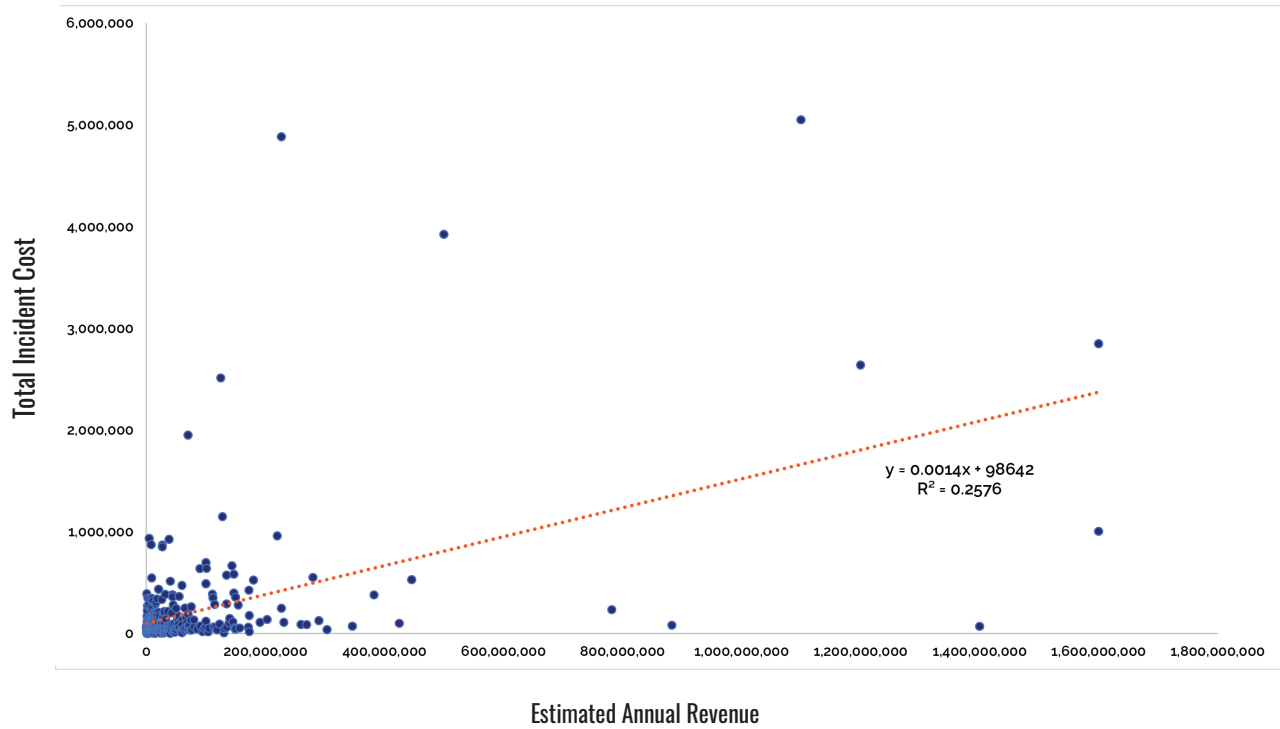


Answer: *Not very much*

Figure 8

Does the incident cost correlate with annual revenue?

5-Years: 2015–2019
(N=358)



Answer: Not very much

Figure 9

